

Bài 2. Vành các lớp thặng dư

A. Tóm tắt lý thuyết

2.1. Quan hệ tương đương - Tập thương

Quan hệ đồng dư theo môđun m là một quan hệ tương đương trên \mathbb{Z} nên nó tạo thành một sự chia lớp trên \mathbb{Z} và ta được tập thương, kí hiệu \mathbb{Z}_m , mà mỗi phần tử của nó được gọi là một thặng dư.

$$\mathbb{Z}_m = \{\overline{0}, \overline{1}, \dots, \overline{m-1}\},$$

trong đó \overline{a} là kí hiệu lớp thặng dư của a .

2.2. Vành \mathbb{Z}_m

Tập hợp \mathbb{Z}_m các lớp thặng dư theo môđun m lập thành một vành với hai phép toán cảm sinh bởi hai phép cộng, nhân trong \mathbb{Z}

$$\begin{aligned}\overline{a} + \overline{b} &= \overline{a+b} \\ \overline{a} \cdot \overline{b} &= \overline{a \cdot b}.\end{aligned}$$

Trong vành \mathbb{Z}_m , lớp thặng dư \overline{a} khả nghịch khi và chỉ khi $\text{UCLN}(a, m) = 1$.
(Lưu ý mọi số nguyên trong cùng một lớp thặng dư có cùng ước chung lớn nhất với môđun).

2.3. Trường \mathbb{Z}_p^*

Tập \mathbb{Z}_m^* các phần tử khả nghịch của vành \mathbb{Z}_m là một nhóm đối với phép nhân của vành \mathbb{Z}_m .
Hơn nữa, nếu $m = p$ là một số nguyên tố thì $\mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{\overline{0}\}$, và \mathbb{Z}_p^* là một trường.

2.4. Hệ thặng dư đầy đủ - Hệ thặng dư thu gọn

Nếu ở mỗi lớp thặng dư của \mathbb{Z}_m ta lấy ra một số nguyên thì ta được một hệ thặng dư đầy đủ môđun m . Nếu ta chỉ chọn các số nguyên đại diện ở các lớp khả nghịch của \mathbb{Z}_m thì ta được một hệ thặng dư thu gọn môđun m .

Hệ thặng dư đầy đủ có m phần tử, còn hệ thặng dư thu gọn có $\varphi(m)$ phần tử.

B. Một số dạng bài toán thường gặp

Dạng 1. Tìm các lớp thặng dư theo môđun m

Phương pháp:

- Sử dụng định nghĩa và tính chất về lớp thặng dư

Ví dụ 1. Hãy tìm các lớp theo môđun 25 trong lớp $\overline{-2} \pmod{5}$.

Giải

Một số nguyên trong lớp $\overline{-2} \pmod{5}$ có dạng $x = -2 + 5t$, $t \in \mathbb{Z}$.

Chia t cho 5 ta được $t = 5k + r$, $0 \leq r < 5$.

Khi đó $x = -2 + 5(5k + r) = 25k + 5r - 2$, $r = 0, 1, 2, 3, 4$.

Cho r thay đổi ta nhận được

$$\overline{x} \pmod{25} = \overline{-2}; \overline{3}; \overline{8}; \overline{13}; \overline{18}.$$

Vậy các lớp thặng dư theo môđun 25 trong lớp $\overline{-2} \pmod{5}$ là:

$$\overline{-2}; \overline{3}; \overline{8}; \overline{13}; \overline{18}.$$

Ví dụ 2. Hãy chỉ ra một hệ thặng dư thu gọn môđun 15 có dạng $4x$.

Giải

Do $\overline{4}$ khả nghịch trong \mathbb{Z}_{15} nên $\overline{4x}$ khả nghịch khi và chỉ khi \overline{x} khả nghịch.

Bởi vậy

$$\overline{x} = \overline{1}, \overline{4}, \overline{7}, \overline{8}, \overline{11}, \overline{13}, \overline{14}.$$

Từ đó ta có thể chọn hệ thặng dư thu gọn môđun 15 đối với x :

$$\{\pm 1, \pm 2, \pm 4, \pm 7\}.$$

Suy ra hệ thặng dư thu gọn môđun 15 có dạng $4x$ là:

$$\{\pm 4, \pm 8, \pm 16, \pm 28\}.$$

Dạng 2. Chứng minh về thặng dư.

Phương pháp:

- Sử dụng định nghĩa và tính chất về lớp thặng dư

Ví dụ 1. Chứng minh rằng: $\bar{3}(\text{mod } 5) \cap \bar{4}(\text{mod } 7) = \bar{18}(\text{mod } 35)$.

Giải

Giả sử x là số nguyên có tính chất $x \in \bar{3}(\text{mod } 5) \cap \bar{4}(\text{mod } 7)$. Thế thì $x = 3 + 5t = 4 + 7u$, $t, u \in \mathbb{Z}$ nào đó.

Bây giờ ta tìm t, u thỏa mãn đẳng thức trên.

$$t = \frac{7u+1}{5} = u + \frac{2u+1}{5}.$$

Đặt $2u + 1 = 5s$, $s \in \mathbb{Z}$ thế thì:

$$u = \frac{5s-1}{2} = 2s + \frac{s-1}{2}.$$

Đặt $s - 1 = 2k$, $k \in \mathbb{Z}$ ta có $s = 2k + 1$ và do đó:

$$u = 2(2k + 1) + k = 5k + 2, \quad x = 4 + 7(5k + 2) = 35k + 18.$$

Vậy $x \in \bar{18}(\text{mod } 35)$.

Ngược lại, dễ nhận thấy $x \in \bar{18}(\text{mod } 35)$ thì $x \in \bar{3}(\text{mod } 5) \cap \bar{4}(\text{mod } 7)$. Do đó

$$\bar{3}(\text{mod } 5) \cap \bar{4}(\text{mod } 7) = \bar{18}(\text{mod } 35).$$

Ví dụ 2. Chứng minh rằng mọi hệ gồm m số nguyên liên tiếp đều lập thành một hệ thặng dư đầy đủ theo môđun m .

Giải

Gọi a_i và a_j là hai số bất kì trong một hệ gồm m số nguyên liên tiếp.

Khi đó $|a_i - a_j| < m$, suy ra $a_i - a_j$ không thể chia hết cho m , hay $a_i \not\equiv a_j (\text{mod } m)$.

Điều này chứng tỏ m số nguyên liên tiếp thuộc vào m lớp thặng dư khác nhau và do đó chúng là một hệ thặng dư đầy đủ theo môđun m .